UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

UNITED STATES OF AMERICA,	**:**	**CASE NO.: 1:15-CR-109**
Plaintiff	**:**	
	:	**JUDGE BARRETT**
vs.	**:**	
	:	**GOVERNMENT'S RESPONSE**
	:	**TO DEFENDANT'S MOTION**
RICHARD STAMPER,	**:**	**TO DISMISS INDICTMENT**
Defendant	**:**	**OR ALTERNATIVELY TO**
	:	**SUPPRESS EVIDENCE**
	:	**SEIZED PURSUANT TO**
	:	**EASTERN DISTRICT OF**
	:	**VIRGINIA SEARCH WARRANT**
	:	
	:	**UNDER SEAL**

The United States, by and through the undersigned, Assistant United States Attorney, Christy L. Muncy, hereby submits its response to defendant's Motion to Dismiss Indictment or Alternatively to Suppress Evidence Seized Pursuant to Eastern District of Virginia (EDVA) Search Warrant (Doc. 33). For the reasons set forth below, the United States respectfully requests defendant's motion be denied.

I. BACKGROUND RELATED TO MOTION

The charges in this case arise from an investigation into a global online forum dedicated to the advertisement and distribution of child pornography through which registered users like Stamper regularly advertised, distributed and accessed illegal child pornography. Beginning in September 2014, Special Agents with the Federal Bureau of Investigation (FBI) operating in the

District of Maryland accessed a website via the Tor Browser.[1] The primary purpose of the website was the advertisement and distribution of child pornography. As of the date the warrant was issued for the website (February 20, 2015, and hereinafter referred to as the "NIT Warrant"), the website contained over 95,000 posts, over 9,000 total topics and hosted over 158,000 members. In addition to posting hardcore child pornographic images, the site also contained forums for the discussion of matters pertinent to child sexual abuse, including methods and tactics offenders use to abuse children, as well as methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes. No adult pornographic images were posted.

The site, hereinafter referred to as "Website A," operated on the anonymous Tor network, which allows a user to mask their actual Internet Protocol (IP) addresses while accessing the internet. In order to access sites on the Tor network, a user must install Tor software. Because of the way Tor routes communications through other computers, traditional IP-address-based identification techniques used by law enforcement who investigate online crimes are not viable. Tor is designed to prevent tracing the user's actual IP address. Accessing a Tor website like "Website A" requires numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon "Website A" without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.[2]

While the FBI was able to view and document the substantial illicit activity taking place on "Website A," investigators faced extreme challenges in identifying the site users engaging in the sexual exploitation of children through the site. Because "Website A" was a Tor website, IP

[1] Background related to the Tor Network is detailed in the Search Warrant Affidavit, made part of the record as Doc. 33-1, Document Under Seal. In the interest of eliminating duplicate filings, the United States will refer to the affidavit at issue by using the docket entry as assigned in Stamper's filings.

[2] Further explanation of this is detailed in the NIT Warrant beginning at Paragraph 7 and continuing through Paragraph 10.

logs which are often found on open-internet sites were not available. Any such user activity logs of "Website A" would contain only the IP addresses of the last computer through which the communications of "Website A" users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information. In order for law enforcement to be able to attain the sort of information that would normally be available from public sources and through ordinary investigative means, the offenders' use of the Tor network necessitated a particular investigative strategy.

Acting on a tip from foreign law enforcement, as well as further FBI investigation, the FBI determined that the computer server that hosted "Website A" was located at a web-hosting facility in North Carolina. In February 2015, FBI agents apprehended the administrator of Website A and seized the website from its web-hosting facility in North Carolina. Rather than merely shut the site down, which would have allowed the over 150,000 users to go unidentified (and not held accountable for their illegal conduct), the FBI interdicted the site and allowed it to continue to operate at a government facility located in the Eastern District of Virginia during a two-week period between February 20, 2015 and March 4, 2015. During that short time, the FBI obtained court approval from the United States District Court for the Eastern District of Virginia to monitor the site users communications and to deploy a Network Investigative Technique ("NIT") on the site (warrant hereinafter referred to as the "NIT Warrant"). The purpose of the NIT was to attempt to identify registered site users (like Stamper) who were anonymously engaging in the continuing sexual abuse and exploitation of children.

As described in detail in the application for the warrant, the NIT consisted of computer instructions which, when downloaded (along with the other content of "Website A") by a registered user's computer, were designed to cause the user's computer to transmit a limited set

of information – the computer's true IP address and other computer-related information (similar to subscriber information for internet service) – that would assist in identifying the computer used to access Website A and its user. (See Exhibit 33-1, Paragraphs 31-27). The search warrant authorization permitted the minimally invasive technique to be deployed when a registered user logged into "Website A" by entering a username and password, while the website was located in the Eastern District of Virginia. (Id., p. 24, Paragraph 32; p. 23, Att. A.).

Law enforcement determined that a person using username "billnyepedoguy" originally registered an account on "Website A" on February 3, 2015. According to the user "billnyepedoguy"'s profile, the user was a NEWBIE Member of "Website A." According to the statistics section of this user's profile, the user "billnyepedoguy" had been actively logged into the website for a total of four hours, one minute and 57 seconds, between February 3, 2015 and March 4, 2015. (See Doc. 32-1, Paragraph 27). IP information obtained from the NIT Warrant resolved back to Richard Stamper. In September 2015, law enforcement agents obtained from this District (Magistrate Judge Stephanie K. Bowman) a search warrant for Stamper's home. That warrant is challenged in Stamper's Motion to Suppress, Document 32.

ARGUMENT

THE MAGISTRATE JUDGE WHO AUTHORIZED THE NIT WARRANT ACTED WITHIN THE AUTHORITY OF RULE 41.

Stamper does not challenge the accuracy of any of the information articulated by law enforcement in NIT Warrant. Rather, he raises an unpersuasive jurisdictional argument. Here, the NIT Warrant was issued by a magistrate judge within the jurisdiction of the U.S. District where "Website A" operated during the period of authorization and, accordingly, the District into which Stamper, a registered user of "Website A," communicated when accessing the website. In any event, law enforcement acted at all times in good-faith reliance upon warrants issued upon

findings of probable cause by neutral and detached magistrates (one in the Eastern District of Virginia and the other in the Southern District of Ohio). The extreme remedies of dismissal or suppression is not justified where, as here, law enforcement diligently sought and received judicial authority for investigative techniques that were necessitated by Stamper's (and others) use of anonymizing technology to criminally exploit children. Accordingly, this Court should deny Stamper's motion in its entirety.

Stamper relies solely on Rules 58 and 59 of the Federal Rules of Criminal Procedure to support his argument the magistrate judge "acted beyond its jurisdiction in the [Eastern District of Virginia]." However, Rule 41(b) grants magistrate judges authority to, among other things, issue warrants for persons or property "outside the district if the person or property is located within the district when the warrant is issued …" (Rule 41(b)(2)); "to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both …" (Rule 41(b)(4)); and to issue warrants "in any district where activities related to the crime may have occurred ..." but within "a United States territory." (Rule 41(b)(5)(a)). Stamper cites no authority for his proposition of dismissal, because none exist.

Furthermore, suppression is not warranted. Stamper blends his reasoning for suppression. On the one hand he argues that the deployment of the NIT constitutes a search of and therefore requires "a proper search warrant." In this instance, a "proper search warrant" was issued by a neutral magistrate judge. Stamper does not challenge any of the factual assertions in the NIT Warrant (or even the residential warrant). On the other hand, Stamper returns to his argument related to jurisdiction in support of suppression. However, even if it were violated, which it was not, "a violation of Rule 41(b) does not 'implicate substantial enough rights to

justify suppression." *United States v. Willoughby*, 2011 WL 6029074, p. 4; *citing United States v. Searp*, 586 F.2d 1117 (6th Cir. 1978); see also *United States v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008) (holding that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause, and with advance judicial approval.")

In this case, the warrant authorized the use of a NIT (a set of computer instructions) which was located on a server in the Eastern District of Virginia at the time the warrant was issued. (See Doc. 33-1, pp. 22-24, 33). Rule 41(a)(2)(A) defines "property" to include both "tangible objects" and "information." The NIT constituted property located in the Eastern District of Virginia when the warrant was issued. Moreover, the NIT was deployed only to users of "Website A" who logged into the website, which was located in the Eastern District of Virginia, with a username and password. Each of those users, like Stamper, accordingly reached into the jurisdiction of the Eastern District of Virginia in order to access the site and the child pornography images and videos therein.

Similarly, Rule 41(b)(4) as referenced above, states that a warrant for a tracking device "may authorize use of the device to trace the movement of a person or property located within the jurisdiction, outside the district, or both," provided, however, that the tracking device is installed within the district. A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Rule 41(a)(2)(E); 18 U.S.C. § 3117(b). In a physical tracking device case, investigators might obtain a warrant to install a tracking device in a container holding contraband, and investigators might then determine the location of the container after targets of the investigation carry the container outside the district. In this case, the NIT functioned in a similar manner. Investigators installed

the NIT in the Eastern District of Virginia on the server that contained the targeted child pornography hidden service. When Stamper logged on and retrieved information from that server, he also retrieved the NIT. The NIT then sent network information to law enforcement. While this network information was not itself location information, investigators subsequently used this network information to identify and locate Stamper. Clearly, the Rules provide authority to issue the warrant.

Additionally, the NIT Warrant was issued by a judge in the district with the strongest known connection to the search: Stamper retrieved the NIT from a server in the Eastern District of Virginia, and the NIT sent his network information back to a server in that district. It was more than reasonable for the EDVA magistrate judge to issue the warrant.

The Good Faith Exception Applies[3]

Even if the Court were to find that the NIT Warrant is deficient, despite Stamper making no arguments related to the strength of probable cause that a crime had been committed, the evidence seized pursuant to that search warrant and the evidence derived from that search is still admissible under the good faith exception to the exclusionary rule. In *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court held that in the absence of an allegation that the magistrate abandoned his detached and neutral role (not argued by Stamper), suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause. *Id.* at 926. Such determinations must be made on a case-by-case basis with suppression ordered "only in those unusual cases in which exclusion will further the purpose of the exclusionary rule." *Id.* at 918.

[3] The United States incorporates as reference additional authority cited in its Response in Opposition to Stamper's Motion to Suppress Evidence Seized Pursuant to the SDOH Warrant.

Stamper does not contend, nor does he cite to any evidence, that the magistrate judge who approved the NIT Warrant abandoned their neutral and detached role. He makes no allegation that any of the information articulated was dishonest or reckless. The NIT Warrant was comprehensive and amply articulated probable cause for the requested technique. Law enforcement officers relied upon that warrant, its fruits, and the subsequent warrant to search Stamper's residence. Accordingly, the Court should find that all of the evidence the defendant requests be suppressed is admissible pursuant to the good-faith exception.

CONCLUSION

For the reasons set forth above, the United States respectfully requests Stamper's motions be denied in their entirety.

Respectfully submitted,
CARTER M. STEWART
United States Attorney

s/Christy L. Muncy
CHRISTY L. MUNCY (KY 88236)
Assistant United States Attorney
221 E. Fourth Street, Suite 400
Cincinnati, Ohio 45202
(513) 684-3711
Christy.Muncy@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Response to Defendant's Motion to Dismiss Indictment or Alternatively to Suppress Evidence (Doc. 33, Under Seal) was served this 22nd day of January, 2016, electronically, upon counsel for defendant.

s/Christy L. Muncy
CHRISTY L. MUNCY (KY 88236)
Assistant United States Attorney